Gültigkeit signierter Dokumente

Von Daniel Muster

Auch elektronisch signierte Dokumente müssen archiviert werden. Dabei sollte die Beweiskraft der Signatur über die Zeit erhalten bleiben.

Bevor elektronisch signierte Dokumente archiviert werden, sollte zuerst geklärt werden, wie ihre Beweiskraft erhalten bleibt. Dabei ist relevant, welche Anforderungen an die Gültigkeit der elektronischen Signatur gestellt werden und wie diese geprüft werden soll.

Art. 2 Bst. c ZertES schreibt zwar für die Gültigkeit der qualifizierten elektronischen Signatur vor, dass bei der Erstellung der Signatur das entsprechende qualifizierte Zertifikat gültig sein muss. Wie aber die Gültigkeit der Signatur zu einem viel späteren Zeitpunkt als bei deren Erstellung geprüft werden soll, wird von den derzeit bestehenden Erlassen beispielsweise in der EU, Deutschland und der Schweiz nicht vorgeschrieben.

Hemmnisse bei der Prüfung

Wenn die Prüfung einer elektronischen Signatur nicht unmittelbar nach der Erstellung erfolgt, dann können unter anderem folgende Ereignisse die Prüfung erschweren oder ohne technische Vorkehrungen sogar verunmöglichen.

➤ **Kompromittierung des Schlüssels:** Wenn zwischen Erstellung und Prüfung der Signatur der Schlüssel kompromittiert worden ist, dann kann ohne weitere technische Vorkehrungen nicht mehr festgestellt werden, wer die Signatur wann erstellt hat. Ein Schlüssel wird dann als kompromittiert betrachtet, wenn die Geheimhaltung des Schlüssels objektiv nicht gegeben ist. Es stellt nämlich keine besondere Schwierigkeit dar, elektronische Dokumente rückwirkend zu datieren und dann zu signieren. Also kann nicht mehr festgestellt werden, ob die Signatur vor der Kompromittierung des Schlüssels oder danach von jemand anderem erstellt worden ist.

➤ **Revokation des Zertifikats:** Ein Zertifikat kann aus irgendeinem Grund zu einem bestimmten Zeitpunkt t für ungültig erklärt (revoziert) werden, beispielsweise weil der Schlüssel kompromittiert worden ist. Nun soll die Signatur später anhand dieses Zertifikats geprüft und dann unter Umständen als gültig erachtet werden, wobei jedoch eine anerkannte Zertifizierungsstelle das fragliche Zertifikat für ungültig erklärt hat.

Wird ein Zertifikat für ungültig erklärt, dann geben die meisten Applikationen nach der Prüfung der Signatur eine Fehlermeldung aus. Dies steht im Einklang mit bestehenden Standards wie etwa RFC 3850. Der Benutzer weiss nun allerdings nicht, ob er der besagten Signatur noch trauen kann oder ob er sich auf die Fehlermeldung der Anwendung verlassen soll.

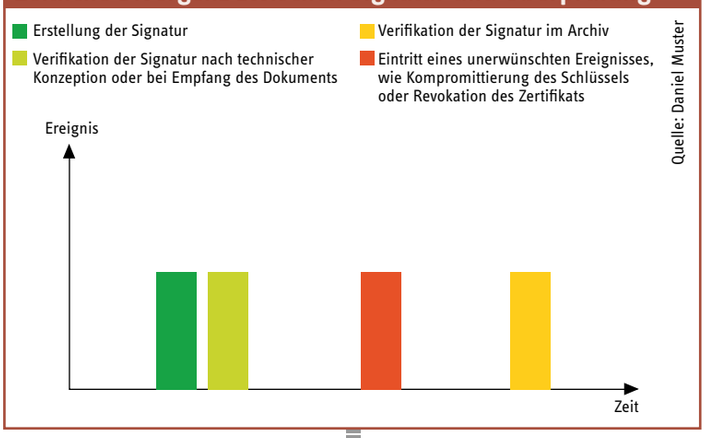
➤ **Ablauf der Gültigkeit des Zertifikats:** Wird eine Signatur nach Ablauf der Gültigkeit des Zertifikats anhand des öffentlichen Schlüssels im besagten Zertifikat geprüft, wird von den meisten Anwendungen ebenfalls eine Fehlermeldung ausgegeben.

Meistens werden nach Ablauf der Gültigkeitsdauer (regulär oder nach einer Revokation) die Zertifikate aus dem Verzeichnis entfernt. Ohne den im Zertifikat enthaltenen öffentlichen Schlüssel können dann auch keine elektronischen Signaturen mehr geprüft werden.

➤ **Schwächung der eingesetzten Verfahren.** Bei den eingesetzten Verfahren gibt es keine Sicherheitsgarantie, dass ein bestimmter Aufwand geleistet werden muss, um sie zu brechen. Deswegen kann es durchaus vorkommen, dass jemand eine Methode findet, wie beispielsweise das bei der Signatur verwendete Verfahren schneller umgangen werden kann.

Grundsätzlich widersprechen sich die technische Konzeption der elektronischen Signatur und die Gesetzgebung. Der technischen Konzeption lag lediglich die Authentisierung (Feststellung des Absenders) zugrunde. Dabei wird angenommen, dass die Erstellung und die Prüfung der Signatur zeitlich nah beieinander liegen. In der Geschäftswelt, insbesondere bei

Zeitliche Divergenz zwischen Signatur und Überprüfung



DER WERKZEUGKASTEN

DTM ODBC Manager 1.0

ODBC-Migrationswerkzeug

www.infoweek.ch/downloads

Wie der Name andeutet, dient der DTM ODBC Manager der Verwaltung der ODBC-Verbindungen. Dabei werden System- wie User-DSNs gleichermassen unterstützt. Als Highlight kann die Export-Funktion bezeichnet werden, womit die Konfigurationsdaten in ein File geschrieben werden. Auf einem anderen Rechner lassen sich diese via Import wieder aktivieren. Migrationen von ODBC-Verbindungen lassen sich so einfach im Point&Click-Verfahren erledigen. Unterstützt werden ausserdem lokale wie auch Remote-Verbindungen. Voraussetzung ist einzig, dass die nötigen Treiber bereits auf dem System vorhanden sind.

der Archivierung, liegen aber die beiden Zeitpunkte möglicherweise über Jahre hinweg auseinander.

Lösung basierend auf Zeitstempel

In den Standards CWA 14171 und RFC 3126 ist ein Lösungsansatz enthalten, der auf Zeitstempeldiensten basiert. Ein Zeitstempel ist eine mit einer qualifizierten elektronischen Signatur und einer Zeitangabe versehene Bescheinigung, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorliegen (Art. 12. ZertES) . Zum Schutz der Vertraulichkeit wird nicht das ganze Dokument dem Zeitstempeldienst zugestellt, sondern nur dessen kryptographische Prüfsumme (Hashwert). Aus diesem Hashwert lassen sich keine Rückschlüsse auf den Inhalt des jeweiligen Dokumentes schliessen.

Möglicher Lösungsansatz

Es gibt grundsätzlich verschiedene Lösungsansätze, wie die Beweiskraft der elektronischen Signatur erhalten werden kann. Eine optimale Lösung hängt von verschiedenen Faktoren ab, wie der Anzahl der zu archivierenden Dokumente und davon, ob alle Dokumente von der gleichen Person signiert worden sind.

Der Lösungsansatz basiert auf Zeitstempel und funktioniert prinzipiell wie folgt:

➤ Zunächst wird das später zu archivierende Dokument (z. B. ein gezeichneter Vertrag) elektronisch signiert und gleichzeitig ein Zeitstempel angefertigt. Damit wird von unabhängiger Stelle belegt, dass die Signatur nicht zu einem späteren Zeitpunkt ans Dokument angefügt wurde.

➤ Im nächsten Schritt wird der Gültigkeitsstatus (meist mittels des OCSP-Protokolls) des Zertifikats beim entsprechenden Aussteller angefragt. Bei einer positiven Antwort des Zertifizierungsdienstanbieters kann gemeinsam mit dem Zeitstempel belegt werden, dass die Signatur beim Empfang des signierten Dokuments gültig gewesen ist.

➤ Danach werden die zur Prüfung der Signatur notwendigen Zertifikate gesammelt, falls sie noch nicht mit der elektronischen Signatur mitgeliefert worden sind.

➤ Aus all diesen Elementen – dem Dokument mit Signatur, dem Zeitstempel, dem Gültigkeitsstatus und den zur Signaturprüfung benötigten Zertifikaten – wird wieder ein Zeitstempel angefertigt. Damit wird belegt, dass dies alles zum besagten Zeitpunkt vorlag.

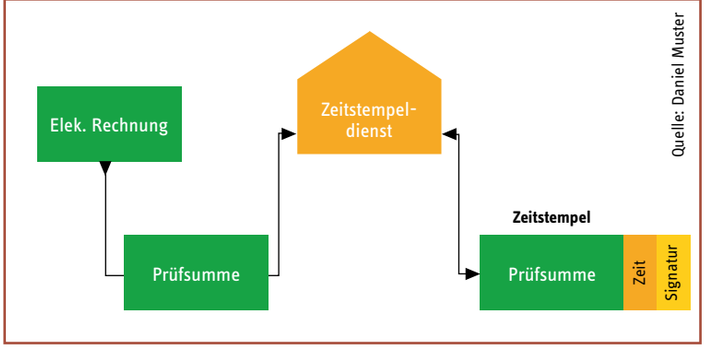
➤ Dieser letzte Zeitstempel wird im Anschluss daran periodisch aktualisiert. Auch die Zertifikate, welche zur Verifikation der Zeitstempelsignatur verwendet werden, haben eine zeitlich limitierte Gültigkeit und müssen deswegen immer wieder aktualisiert werden.

Fazit

Ein Verfahren, wie die Beweiskraft elektronisch signierter Dokumente erhalten bleibt, wird von den bestehenden Erlassen bisher nicht geregelt. Es gibt aber Lösungsansätze dazu, welche auf international anerkannten Standards basieren. Produkte für einzelne Prozesse sind grundsätzlich vorhanden, müssen aber zum Teil noch zusammengeführt und integriert werden.

Daniel Muster arbeitet in der anwendungsorientierten Forschung und Entwicklung an der Hochschule für Technik Zürich (HSZT), 8021 Zürich.

Lösungsansatz basierend auf Zeitstempel



Quellen

D. Muster	Digitale Unterschriften und PKI, März 2006, ISBN 3-9522387-3-3, HSZ-T
ZertES	Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)
[TAV]	Technische und Administrative Vorschriften des BAKOM vom 6. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)
CWA 14171	CEN (www.cenorm.be), General Guidelines for electronic signature verification
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
RFC 3126	Electronic signature formats for long term electronic signature
RFC 3850	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling